79-260

DCI SCHEDULING ITEM

DATE RECEIVED: 27 September 1979 DATE OF EVENT: Tuesday, 15 Jan 80

1. INFORMATION REGARDING THE APPOINTMENT: SUSPENSE: 11 October 1979

a. Source: Tel: Memo ~~xxx~~ Fm: Stephen T. Walker

b. Type of event: Keynote address by DCI

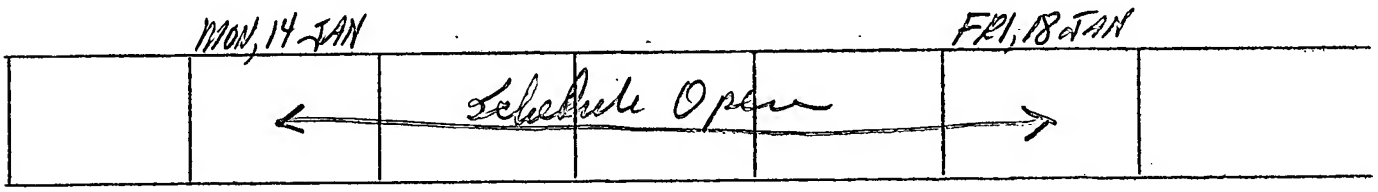
c. Special occasion: Seminar on DoD Computer Security Initiative

d. Date/Time: 0930-1000 hours, Tuesday, 15 January 1980

e. Location: National Bureau of Standards, Gaithersburg, MD

f. Significant info: Topic: Computer Security Interests in Intelligence Community

2. SCHEDULE:



3. RECOMMENDATIONS:

	Schedule	Regret	Remarks
AIDE		Re	Estimate return from Far East trip & be 11 or 12 Jan. You'll need time to "catch up" on business. Recm DDA.
EA			

4. DCI DECISION:

a. SCHEDULE_____ NO_____ SEE ME_____

b. ADDITIONAL ATTENDEES_____

c. PASS TO: DDCI_____ D/DCI/IC_____ D/DCI/NI_____ OTHER_____

STAT

5. AIDE FINAL ACTION: Jerry - advise [redacted] - done, he will greet

STAT [redacted]

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301

COMMUNICATIONS, COMMAND,
CONTROL, AND INTELLIGENCE

IC staff (Computer Sec.)

20 SEP 1979

STAT MEMORANDUM FOR

SUBJECT: Computer Security Seminar, 15-16 January 1980

I would like to invite Adm Turner to be the Keynote Speaker at the Seminar on the DoD Computer Security Initiative to be held at the National Bureau of Standards, Gaithersburg, Maryland, on 15 January 1980.

This is the second in a series of Seminars on the DoD Computer Security Initiative Program to inform the computer industry and the general public of the interest that the DoD has in trusted computer systems, and the progress in this field that has been made by the DoD research community in recent years. These seminars are a major part of the Initiative's efforts to encourage the computer industry to develop high integrity computer systems for use by the DoD and the rest of their customer base.

Attachment 1 is the brochure that was distributed for the first seminar held on 17-18 July 1979.

Attachment 2 is a tentative program plan for the 15-16 January 1980 seminar.

Attachment 3 is a copy of Dr. Dinneen's Keynote Address at the first seminar.

The seminar is being held at the National Bureau of Standards at Gaithersburg, Maryland, because of their excellent conference facilities and the strong interest that NBS has in the computer security area.

Attendance at the first seminar consisted of approximately

100 from Government (11 DoD organizations, 17 Federal organizations)
100 from 10 major computer manufacturers (IBM, Honeywell, Univac, DEC, etc)
100 from system developers and users

Adm Turner's presentation should be approximately one half hour and would be scheduled from 0930 to 1000 A.M., if that is convenient.

Stephen T. Walker

Stephen T. Walker
Chairman
Computer Security Technical
Consortium

Attachments 3

SEMINAR ON THE DEPARTMENT OF DEFENSE COMPUTER SECURITY INITIATIVE PROGRAM

July 17-18, 1979

NATIONAL BUREAU OF STANDARDS
Gaithersburg, Maryland

SPONSORED BY:

U.S. Department of Defense
Office of the Secretary of Defense
Under Secretary of Defense for
Research and Engineering
Information Systems Directorate

U.S. Department of Commerce
National Bureau of Standards
Institute for Computer Sciences
and Technology
Center for Programming Science
and Technology

ABOUT THE SEMINAR

The objective of this seminar is to acquaint computer system developers and users with the status of the development of "trusted"* ADP systems within the Department of Defense and the current planning for the integrity evaluation of commercial implementations of these systems. The seminar will present an overview of a number of topics essential to the development of "trusted" ADP systems. Much of the material to be presented will be of a technical nature that is intended for computer system designers and software system engineers. However, the sophisticated computer user in the Federal government and in private industry should find the seminar useful in understanding security characteristics of future systems. This is the first in a series of technical seminars; future sessions will include detailed presentations on:

Security Kernel Design Experience

KSOS, KVM, SCOMP, Secure Unix Prototypes, Multics AIM

Specification and Verification Techniques

Secure System Applications

* A "trusted" ADP system is one which employs sufficient hardware and software integrity measures to allow its use for simultaneously processing multiple levels of classified and/or sensitive information.

ABOUT THE D COMPUTER SECURITY INITIATIVE

The Department of Defense (DoD) Computer Security Initiative was established in 1978 by the Assistant Secretary of Defense for Communications, Command, and Control and Intelligence to achieve the widespread availability of "trusted" ADP systems for use within the DoD. Widespread availability implies the use of commercially developed trusted ADP systems whenever possible. Recent DoD research activities are demonstrating that trusted ADP systems can be developed and successfully employed in sensitive information handling environments. In addition to these demonstration systems, a technically sound and consistent evaluation procedure must be established for determining the environments for which a particular trusted system is suitable.

The Computer Security Initiative is attempting to foster the development of trusted ADP systems through technology transfer efforts and to define reasonable ADP system evaluation procedures to be applied to both government and commercially developed trusted ADP systems. This seminar is the first in a series which constitute an essential element in the Initiative's Technology Transfer Program.

The Institute for Computer Sciences and Technology, through its Computer Security and Risk Management Standards program, seeks new technology to satisfy Federal ADP security requirements. The Institute then promulgates acceptable and cost effective technology in Federal Information Processing Standards and Guidelines. The Institute is pleased to assist the Department of Defense in transferring the interim results of its research being conducted under the Computer Security Initiative.

GENERAL INFORMATION

Registration

A registration fee of $25 is being charged to all attendees to help defray the costs of conducting the Seminar. Advanced registration is requested in order to complete local arrangements. Please send the enclosed registration form along with your registration fee (checks made payable to COMPUTER SECURITY INITIATIVE, no purchase orders, please) to:

Mr. Stephen T. Walker
Department of Defense
OSD (C3I), Room 3B252
Pentagon
Washington, D.C. 20301

The Seminar registration desk will be open at NBS beginning at 8:30 a.m., July 17, outside the Green Auditorium.

Housing

The Sheraton-Silver Spring, 8727 Colesville Road, Silver Spring, Maryland 20910, is designated the official headquarters hotel for the Seminar. A block of rooms at special rates ($34 single; $36 twin) has been reserved at the Sheraton-Silver Spring for Seminar attendees. A reservation card is enclosed in the announcement, and this should be forwarded directly to the Sheraton-Silver Spring at the earliest opportunity, and no later than June 25, 1979. After that date all rooms in the block which have not been reserved will be released for general sale at the regular prevailing rates of the hotel. Please use the reservation card rather than calling in your reservation, as this identifies you as a participant and eligible for the special rate.

Transportation

Daily bus service will be provided between the Sheraton-Silver Spring Hotel and the National Bureau of Standards. For those attendees arriving by air, the Sheraton-Silver Spring is accessible by regular airport limousine service from Dulles and National Airports.

Transportation will be provided to the airports from NBS at the conclusion of the meeting on Wednesday.

Luncheons

Fixed-menu lunches, included as part of the Conference activities, will be served in the NBS Cafeteria.

Meeting Rooms

All technical sessions will be held in the Green Auditorium of the Administration Building, National Bureau of Standards, Gaithersburg, Maryland.

For Further Technical Information:

Stephen T. Walker
(202) 695-3287

For Further General Information:

Dennis K. Branstad
(301) 921-3861

Place in envelope with check for $25 made payable to "COMPUTER SECURITY INITIATIVE SEMINAR"

Stephen T. Walker
Department of Defense
OSD (C3I), Room 3B252
Pentagon
Washington, D.C. 20301

For Information Call 202-695-3287

Approved For Release 2009/04/20 : CIA-RDP05S00620R000501230036-2

Computer Security Initiative Seminar
National Bureau of Standards
Gaithersburg, Maryland
July 17-18, 1979

REGISTRATION FORM

Name _____

Organization _____

Street Address _____

City _____ State _____ Zip _____

Telephone _____

Registration Fee Enclosed—$25

FOR OFFICE USE ONLY

Ck. _____
Csh. _____
Date _____
By _____

Computer Security Initiative Seminar

Sheraton-Silver Spring
8727 Colesville Road
Silver Spring, Md 20910 Telephone (301) 589-5200

Guest Room Reservation Request

Name _____

Address _____

City _____ State _____ Zip _____

RESERVATIONS MUST BE RECEIVED not later than two weeks prior to arrival date, and ROOMS WILL BE HELD ONLY UNTIL 6 P.M. ON DATE OF ARRIVAL, unless guaranteed in writing. CHECK OUT TIME IS 1 P.M.

ARRIVAL DATE_____HOUR A.M. P.M. DEPARTURE DATE_____HOUR A.M. P.M.

☐ Singles $34 ☐ Twins $36 (Special Conference Rate) All Rates Plus Md. Tax
Free Parking—Year Round Pool—Supper Club

Approved For Release 2009/04/20 : CIA-RDP05S00620R000501230036-2

Place
Stamp
Here

BUSINESS REPLY MAIL

The Sheraton-Silver Spring
8727 Colesville Road
Silver Spring, Maryland 20910

Attention: Reservations

PROGRAM

SEMINAR ON
THE DEPARTMENT OF DEFENSE

COMPUTER SECURITY INITIATIVE PROGRAM

July 17, 1979

8:30 am	Registration *at National Bureau of Standards*
9:15	Opening Remarks James H. Burrows, Director *Institute for Computer Sciences and Technology* *National Bureau of Standards*
9:30	Keynote Address "Computer Security Requirements in the DoD" Honorable Gerald P. Dinneen *Assistant Secretary of Defense for Communications, Command, Control and Intelligence*
10:00	DoD Computer Security Initiative Program Stephen T. Walker *Chairman, DoD Computer Security Technical Consortium*
11:15	Coffee Break
11:30	Protection in Operating Systems Edmund Burke *MITRE Corporation*
1:00 pm	Lunch
2:00	Kernel Design Methodology LT. COL. Roger Schell, USAF *Naval Post Graduate School*
3:15	Break
3:30	Formal Specification and Verification Peter Tasker *MITRE Corporation*
4:30	Adjourn

July 18, 1979

9:00 am	Secure System Developments Kernelized Secure Operating System (KSOS) Dr. E. J. McCauley *Ford Aerospace and Communications Corporation* Kernelized VM-370 Operating System (KVM) Marvin Shaefer *System Development Corporation* Secure Communications Processor Matti Kert *Honeywell Corporation*
11:00	Coffee Break
11:15	Secure System Applications John Woodward *MITRE Corporation*
1:00 pm	Lunch
2:00	System Evaluation Process Stephen T. Walter
3:30	Adjourn

NOTES

NOTES

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

THIRD CLASS MAIL
BULK RATE

Approved For Release 2009/04/20 : CIA-RDP05S00620R000501230036-2

TENTATIVE PROGRAM
(All presentation titles are tentative)

Seminar on the Department of Defense Computer Security Initiative

National Bureau of Standards
Gaithersburg, Maryland

January 15

Opening Remarks

Keynote Address
"Computer Security Interests in Intelligence Comm"
Adm Stansfield Turner
Director of Central Intelligence

"Computer Security Interests in the Services"
Dr. Robert Hermann
Under Secretary of the Air Force for Research and Development

"Computer Security Interests in the Federal Government"
Mr. James Burrows
Director, Institute for Computer Science and Technology
National Bureau of Standards

"Computer Security Interests in the Private Sector"
Mr. Ed Jacks
General Motors Corporation

Lunch

"Computer Security Impacts on Near Term Systems"
Mr. Clark Weissman
System Development Corporation

"Computer Security Impacts on Future System Architectures"
Dr. Jerome Saltzer
MIT

"The Manufacturer's Perspective: What the Industry Would Like to Hear from the Government on Computer Security"
Mr. Theodore M. P. Lee
Univac Corporation

"What the Industry Should Expect to Hear from the Government on Computer Security"
Mr. James P. Anderson
Consultant

January 16 (Two Parallel Sessions)

I. Technical Session - Green Auditorium

Tutorial Review of progress in DoD research community on building and applying trusted operating systems. Details on:

- Kernelized Secure Operating System (KSOS)
- Kernelized VM370 Operating System (KVM)
- MULTICS
- SCOMP
- Applications

Panel Discussion and question and answer period

II. Requirements Session - Red Auditorium

Range of Applications within DoD and Beyond
R. Stockton Gaines
Rand Corporation

DoD Policy Issues
Eugene Epperly
Deputy Under Secretary of Defense
(Security Policy)

Practical Experiences with Approving Trusted Systems

STAT [redacted]
DIA

Perspectives on Evaluation Process with DoD and Beyond
Robert Campbell
Consultant

KEYNOTE ADDRESS
on
COMPUTER SECURITY REQUIREMENTS IN THE DOD

by

DR. GERALD P. DINNEEN
Assistant Secretary of Defense (C^3I)

Welcome to the first seminar on the Department of Defense Computer Security Initiative. The goal of this initiative is (Slide available if you would like) to achieve the widespread availability of trusted computer systems. By "trusted", we mean systems with sufficient hardware and software integrity measures to allow their use for simultaneously processing multiple levels of classified or sensitive information. By "widespread" we imply the use of commercially developed trusted ADP systems whenever possible.

Let me begin with the understanding that today's computer systems in the DoD are secure in the physical, administrative, and procedural sense. We know how to treat computers like black boxes and lock them in physically secured facilities. However, with only a few exceptions, we are not able to rely on the integrity of the hardware and software components of our computers to properly isolate users from each others' data. We have therefore been forced to clear all users of a particular system to the same access level to prevent hardware or software failures from resulting in security violations.

As our computers become linked in worldwide data networks we can no longer afford to clear everyone to the highest level in the network. Even if we could, the "need to know" principle limits access to information to those who need it to perform their specific responsibilities.

"Information Exchange" is the key to success in any endeavor. In the DoD, and in particular in C^3I situations, the ability to accurately convey information is essential. Computers are becoming involved in every aspect of our information exchange activities. Until we can trust computers to accurately control access to critical information, our information exchange efforts will be seriously hindered. We have many ongoing programs which have strong requirements for trusted computer systems:

- WWMCCS has had a long stated requirement.
- The intelligence community has strong needs within its own community as well as in its interface to the rest of the national security community.
- Even our logistics and financial communities are faced with serious problems through the lack of trusted system developments.

Let me use as an example a hypothetical, but typical, automated text message handling problem. A nominal DoD message handling system might have twenty-five information sources and as many as two hundred distribution points. Some number of the information sources, say five, claim they cannot allow access to their information because there is not assurance that the information will not be sent to ten distribution points which are not cleared either for level or "need to know" access in all instances. To resolve this dilemma we have a number of possible solutions including:

1. Clear all distribution points to "too high" a level;

2. Set up multiple systems and somehow deal with the inherent problems such as maintaining multiple copies of data bases, plus the additional duplicate system expenses;

3. Deny some users access to data they need to do their jobs; or,

4. Build the message handling application on a trusted system base to maintain whatever access control processes are required.

Clearly, if possible, the last solution to build a trusted system is the most desirable and effective.

This is just one example of the problems we currently face, but I do not believe we should limit the computer security issue to only analyzing problems within existing programs. In a very real sense, the lack of trusted computer systems has limited to a degree the way we think about using computers. We have been so inhibited by our inability to trust computers that in many sensitive areas, our information exchange process has been warped. The existence of high integrity operating systems will create a dramatic shift in our ability to provide the right information to the right people at the right time.

In the next two days you will hear about technological developments which we feel will soon allow us to trust computer systems in many of our sensitive information handling environments. The developments you will hear about should not be interpreted as the ultimate answer but rather as a reasonable beginning. We feel confident that they are moving us on the path toward generally available trusted systems. I wish to emphasize that we do not today claim to have the solutions to all the problems. We do believe that the technology needed to build trusted systems is becoming available and we would like to encourage the development of trusted systems.

If we are to have widely available systems (that is, other than DoD developed special systems) we must involve the computer industry in this process. But before the industry will invest much effort in trusted systems, they must be convinced that such systems are reasonable for use on broader government and private sector sensitive information handling applications. Dr. Ware will address some of these beyond the DoD requirements in a few minutes. I want to emphasize that while we in the DoD may have a slight lead in understanding the nature of our sensitive information handling problems because of a long history of handling classified information, the general requirements of the rest of the Government and of the private sector are very similar to the kinds of problems we are trying to address. We hope that our efforts in this area may help to create the kind of trusted computer systems that can be used by anyone with sensitive information to process.

The program you will be hearing about in the next two days is not a Government R&D program involving grants to develop trusted computer systems. We believe that there will be sufficient market for trusted computer systems that the computer manufacturers will build high integrity trusted systems without the incentive for government development dollars. The Government R&D investment in this program is intended to demonstrate new approaches to solving the computer security problem but, beyond the initial demonstrations, our funds will be concentrated in trusted system applications.

Building computer hardware and software systems is a very complex process that the Government is no longer directly involved in except for special purpose systems that are unique to our needs. The large majority of our computer systems are purchased from the commercial market place. We realize that, if we are to achieve widespread availability of trusted systems, they must come from this same source. The DoD cannot afford, just for the sake of having trusted computer systems, to develop its own general purpose hardware and software systems. Further, we cannot afford to pay for special security related modifications to existing systems, with all the expensive long term maintenance implications. Nor do we believe that the manufacturers will spend their own IR&D funds to develop systems suitable for use just in the DoD market place.

Therefore, it has been an essential part of our computer security R&D program, to develop systems that are suitable for use in a wide variety of sensitive information handling environments (DoD, Federal Government, Private Sector), using software and hardware development techniques which are state-of-the-art and suitable for adoption by the computer manufacturers.

To the extent that we are successful, the manufacturers will find a much larger market for their trusted systems than just the DoD and the users of computers in sensitive information handling environments will find a significant improvement in the integrity of commercially available computer systems.

The technology for building computer hardware and software systems has always been an open, freely discussed and highly competitive field. The fact that we have made such significant advances in this field is due in large part to the openness which surrounds it. The basic technologies which we are employing to build and verify trusted computer systems (the technologies which you will hear about later today) are products of this open development environment. Yet as we employ these techniques on systems which will be used to protect sensitive information from improper disclosure or modification, we encounter a serious dilemma.

We know that no single security measure or combination of measures is 100% failure proof. Trusted computer systems while offering significant new capabilities to our computer usage also add an additional set of vulnerabilities to the overall security posture. We must recognize that, as with all other security mechanisms, there is always a potential for vulnerabilities with our hardware and software systems which we will have to protect by means of the physical and administrative measures that surround these systems.

We are going to have to draw a fine line between the openness with which we discuss computer systems development in general and the information restrictions we use to protect the potential vulnerabilities that may exist in the integrity measures of a particular system. We will have to develop procedures for protecting security relevant design and implementation details while not inhibiting general technological advances. I want to stress that this is not just a Department of Defense or U.S. Government problem but one which all of us face if we wish to develop or use high integrity systems. The solution to what information should be freely available and what should be restricted, and from whom it should be restricted, will not come easily and deserves the careful attention of all interested parties. I ask your help in arriving at a suitable solution.

In order to ensure that we can make the most effective use of trusted computer systems, we are attempting to establish an efficient and consistent evaluation process for determining the integrity of computer systems and the environments for which a particular system will be suitable. We hope to convey to you in the next two days some of the important technical elements that will influence this evaluation process. We are actively working toward establishing this evaluation process, though, I must emphasize, it may take some time to achieve our full objectives.

We feel it is essential to begin the dialogue on trusted computer systems with the computer system developers and major users immediately in order to ensure the earliest availability of these systems. This seminar is intended to initiate that dialogue. Our needs in this area are real and serious and we are eager to use trusted computer systems in existing and broad new applications as soon as they are available.